Qualifier Exam in Information Security

Spring 2011

You have to answer at least one question in each section and get at least 60 points to pass the exam.

1 Network Security

Problem 1, 10 points.
Describe push-back and trace-back mechanisms. What attacks are they designed to address? How can they be implemented in real networks? Why have they not been deployed?

Problem 2, 10 points.
What are ”session hijacking” (sidejacking) attacks? What solution has been most widely suggested to defeat such attacks? Why do many websites not automatically use this technique?

Problem 3 , 10 points.
After feeling ill for a number of weeks, you decide to see a doctor. Having spent significant time overseas, the doctor tests you for a rare but dangerous disease (it infects one out of every million people on the planet). The doctor uses a very accurate test (99% accurate) to determine whether or not you are infected with the disease; unfortunately, your test came back positive. What is the likelihood that you are actually infected? How many false positives will this test catch? Should you ask the doctor to test you again? What are the implications of this medical question upon information security?

2 System and Software Security

Problem 4, 10 points.
The RSA SecurID token is used for two-factor authentication by a large number of enterprises. The New York Times reported on March 18 that hackers may have stolen sensitive data from RSA computers that could lead to potential compromise of SecurID tokens.

Discuss a possible implementation for SecurID like tokens and how they are used in remote authentication. Identify the threats that can be handled when a SecurID like token is used as an additional authentication factor. Also, describe what kind of data may have been stolen by hackers which could result in the compromise of this token-based authentication scheme.

Problem 5, 10 points.
In a recently proposed system, remote users are allowed to submit untrusted code that can operate on sensitive data stored on a trusted Cloud as long the following holds: (1) the untrusted program can be confined while it executes so it is not able to send data outside the Cloud via the network, and (2) a trusted program running on the Cloud is able to examine and possibly modify the output produced by the untrusted program before it is returned to the user.

How can an untrusted program be confined on a system? Explain what operating system mechanisms will be necessary for such confinement and use example systems to illustrate them.

Also, many privacy persevering systems explore techniques that transform sensitive data from it is disclosed to reduce the likelihood that privacy is violated. Discuss two such techniques and their strengths and limitations.

Problem 6, 10 points.
A recent news story mentioned that William Lynn, who is United States Deputy Secretary of Defense, met executives at Intel and Microsoft to discuss what these companies could do to help build computer systems that can more effectively resist cyber attacks. As a computer security expert, how do you make sense of such a story? More specifically, answer the following.

As a hardware vendor, what does Intel do to enable security and what more can it do so we can build computer systems that can resist the kinds of attacks referred to by Lynn?

Similarly, what can an OS vendor like Microsoft do for the same? Provide technical justifications for your suggestions.

3 Cryptogrphy

Problem 7, 10 points.
You have two encryption schemes, which are designed to encrypt messages of n bits, where $n \geq 1$ is some fixed integer. You know that only one of the two schemes is provably secure (IND-CPA) under some well-studied assumption, but you don't know which one. Describe how will you encrypt an n-bit message securely (IND-CPA). Try to come up with the most efficient scheme. Justify security of your approach. You don't have to give a formal proof, but try to come up with a convincing argument.

Problem 8, 10 points.
A typical ciphertext of a message M created with hybrid ElGamal scheme has the following form: $(g^r, g^{xr} \cdot K, \mathcal{SE}_{H(K)}(M))$, where g is a public generator of a cyclic group of prime order p, g^x is the receiver's public key, r is a random element of Z_p, K is a random group element chosen by the sender, $\mathcal{SE}$ is the encryption algorithm of some secure symmetric encryption scheme, and H is a public hash function, modeled in the security proof as a random oracle. One can show that such a scheme is IND-CPA if H is a random oracle, the CDH problem is hard in the underlying group and the symmetric scheme is IND-CPA. Suggest a modification, which allows on to decrease the size of the ciphertext without compromising security. You don't have to give a formal proof, but try to come up with a convincing security argument.

Problem 9, 10 points.
One can show that $H(K||M)$ is a secure MAC in the random oracle model.
Show that this MAC is insecure in practice, i.e. when H is SHA-1 (or any other collision-resistant hash) used in the Merkle-Damgard transform.